Secure Element –
Protecting Your Digital Life

Dr. H. Karen Lu
July 27, 2016
We enable our clients to bring trusted and convenient digital services to billions of people

- €3.1bn 2015 Revenue
- 14,000+ Employees
- 3,000 R&D Engineers
- 4000+ Patents
- 117 Nationalities of Our Employees
- 180+ Countries Where Our Clients Are Based
- 30,000+ End Users Benefit From Our Solutions
- 3000+ Financial Institutions
- 450 MNOs
- 80+ Government Programs
Amazing digital future for man and machines

- Internet of Everything
  - We use our smart phones, tablets, laptops in every aspect of our lives
  - Our smart homes anticipate our needs
  - We live in smart cities
  - Our data and robot intelligence live in the cloud
Great new convenience and productivity

- Our automobiles drive themselves
- Our drudgework “chores” disappear
- Automatic backup of *everything*
- We can be productive while riding in our cars
- CO₂ emissions dramatically reduced
Terrifying vulnerabilities

Many things are automated
- Cities, homes, finances, appointments…
- Our smart homes and online services know everything about us

Automation may introduce vulnerabilities
- Many of today’s systems have little protection
  - e.g., power grid, HVAC, water supply
- What about state-sponsored or terrorist group attacks?

What about our privacy?
- How do we keep our personal data away from wrongdoers?
You are not as safe as you think

“In the space of one hour, my entire digital life was destroyed.”
- Mat Honan 08.06.12  8:01 PM

Theft of identities and personal information retains top spot, accounting for 53% of data breaches; healthcare and government overtake retail as most-targeted sectors

AMSTERDAM – February 23, 2016 — Gemalto [Euronext NL0000400653 GTO], the world leader in digital security, today released the latest findings of the Breach Level Index, revealing that 1,673 data breaches led to 707 million data records being compromised worldwide during 2015.

NUMBER OF BREACH INCIDENTS BY TYPE

- Identity Theft: 53%
- Financial Access: 22%
- Existential Data: 11%
- Account Access: 11%
- Nuisance: 3%
World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated with July 2020)

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
What does it take to break a password?

<table>
<thead>
<tr>
<th>Password</th>
<th>Combinations</th>
<th>Class A</th>
<th>Class B</th>
<th>Class C</th>
<th>Class D</th>
<th>Class E</th>
<th>Class F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>100</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>3</td>
<td>1,000</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>4</td>
<td>10,000</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>5</td>
<td>100,000</td>
<td>10 Secs</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>6</td>
<td>1 Million</td>
<td>1½ Mins</td>
<td>10 Seconds</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>7</td>
<td>10 Million</td>
<td>17 Mins</td>
<td>1½ Mins</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>8</td>
<td>100 Million</td>
<td>2¾ Hours</td>
<td>17 Mins</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>9</td>
<td>1,000 Million</td>
<td>28 Hours</td>
<td>2¾ Hours</td>
<td>17 Mins</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Password</th>
<th>Combinations</th>
<th>Class A</th>
<th>Class B</th>
<th>Class C</th>
<th>Class D</th>
<th>Class E</th>
<th>Class F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3,844</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>3</td>
<td>238,328</td>
<td>23 Secs</td>
<td>&lt; 3 Secs</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>4</td>
<td>15 Million</td>
<td>24¾ Mins</td>
<td>2½ Mins</td>
<td>15 Secs</td>
<td>&lt; 2 Secs</td>
<td>Instant</td>
<td>Instant</td>
</tr>
<tr>
<td>5</td>
<td>916 Million</td>
<td>1 Day</td>
<td>2½ Hours</td>
<td>15¾ Mins</td>
<td>1¼ Mins</td>
<td>9 Secs</td>
<td>Instant</td>
</tr>
<tr>
<td>6</td>
<td>57 Billion</td>
<td>66 Days</td>
<td>6½ Days</td>
<td>16 Hours</td>
<td>1½ Hours</td>
<td>9½ Mins</td>
<td>56 Secs</td>
</tr>
<tr>
<td>7</td>
<td>3.5 Trillion</td>
<td>11 Years</td>
<td>1 Year</td>
<td>41 Days</td>
<td>10 Hours</td>
<td>58 Secs</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>218 Trillion</td>
<td>692 Years</td>
<td>69½ Years</td>
<td>7 Years</td>
<td>253 Days</td>
<td>25½ Days</td>
<td>60½ Hours</td>
</tr>
</tbody>
</table>

We have to look for better solutions…

http://www.lockdown.co.uk/
How do we protect our digital life?
Secure Element (SE)

- Smart Card (IC Card) was invented in 70’s.

- Tamper-resistant platform
  - With an embedded microprocessor
  - Secure memories; ROM, Flash, RAM
  - Secure hardware and secure firmware/software
  - Hardware cryptographic engine
  - Host application, confidential data, and cryptographic keys

- Secure hardware
  - Sensors to detect power supply fluctuation, clock manipulation, physical tampering.
  - Circuit designed to prevent side channel attacks (EM, power draw, timing)
  - Automatic shut-down and data erased when attack detected

- Secure personalization and deployment
  - Remotely manage the life cycle of digital credentials

- Multiple form factors and means of communications
Secure Elements

Detached SE
- Via NFC
- Via Bluetooth
- Via contact

Semi-detached SE
- MicroSD
- UICC

Embedded SE
- eSE
- TEE
Applications

- Strong authentication
- Secure banking
- Trusted identity for mobile phones and remote machines
- Digital signature
- Data encryption and decryption
  - Crypto keys are strongly protected
- Internet of Things (cars, smart homes, …)
- Many more and coming…
Classical Smart Card Applications
Subscriber identification module (SIM)

- Used to identify and authenticate subscriber

Inside SIM

- ICCID: integrated circuit card identifier – internationally identified
  - Network specific information

- IMSI: International mobile subscriber identity
  - Uniquely identify the SIM card in its operator network

- Authentication key
  - *Authenticate the mobile device to the network*

- Preferred networks – for roaming

- SMS messages and contacts (before smart phones)
Identification (ID) Cards

❖ Adoptions
  ❑ Government
    ❖ e.g. Personal Identification Verification (PIV)
  ❑ Enterprise
  ❑ Health care

❖ Usage
  ❑ Physical access
  ❑ Logical access
    ❖ Login to computer networks
    ❖ VPN
  ❑ Encryption / decryption documents, emails
  ❑ Digitally signing documents, emails
Banking card

- Magnetic strip credit cards are easy to duplicate

- Smart card is secure and tamper resistant

- Practically impossible to duplicate a smart card
  - Banks trust it!

- Chip card is widely used around the world

- Finally arrived in America...
What is EMV?
EMV

- EMV is a technical standard for smart payment cards, payment terminals, and automated teller machines (ATMs).
- EMV stands for Europay, MasterCard, and Visa.
  - Introduced in 1994
- The standard is now managed by EMVCo
  - Consortium of Visa, Mastercard, JCB, American Express, China UnionPay, and Discover
Why EMV?

✦ Improve fraud protection
✦ Achieve global interoperability
✦ Reduce transaction cost
✦ Improve acceptance with offline transactions
Important security measures in EMV

- Card Authentication (CAM)
  - Is the card genuine?
  - Using asymmetric key cryptography
  - Against counterfeit fraud

- Cardholder Verification Method (CVM)
  - CVM is method used to ensure that a credit card being used is in the possession of its owner
  - EMV supports several CVMs

- Risk management and authorization
  - Authorization Request Cryptogram (ARQC)
  - Control financial risks
EMV Transaction (Online – no CVM)

Credits to Jack Jania of Gemalto for this and the following EMV slides
EMV chip transaction – Online

- Transaction initiation: POS and card exchange data
  - Track 2 equivalent data
  - Card settings and capabilities
  - Transaction data (amount, currency, date, etc)
  - ...

- Card data
  - Amount, currency, ...

- CVM

- Card authN

- Issuer authorization system
EMV chip transaction – Online

- Card generates an Authorization ReQuest Cryptogram (ARQC).
- ARQC is the encryption of card and terminal data using a secret key specific to that card. This key can be retrieved by the issuer authorization system.
- ARQC is a DYNAMIC cryptogram: it is different for each transaction.
EMV contact transaction – Online

- Authorization request is sent to the issuer authorization system
  - Same data as for magstripe transaction
  - Additional EMV data
EMV contact transaction – Online

- The authorization system performs risk management
- It also checks the validity of the ARQC by recalculating it using:
  - the data transmitted in the authorization request
  - the secret key associated to that card
- If the ARQC is validated, the card is considered genuine, and there is a guarantee that the transaction data have not been tempered with (amount, …)
EMV contact transaction – Online

- Card authentication is based on DYNAMIC data (ARQC) generated by the card secret key

- Card secret key cannot be retrieved from a card and duplicated onto another card
EMV contact transaction – Online

Issuer host generates an authorization response

- Response may include an Authorization ResPonse Cryptogram that authenticates the issuer and the issuer decision. The card may validate the ARPC before giving its final decision.
EMV contactless and NFC transactions – Online

- Contactless and NFC transactions offer the same level of security as contact transactions.
- Contactless and NFC devices leave the field before the authorization response is received by the POS. Issuer actions can be performed:
  - Card: during the next contact transaction
  - Mobile phone: using the OTA (over-the-air) channel
Modern Applications
Emerging Applications

- National eID
- Citizen passport
- Health care card
- Online applications
- Mobile Payment

Southwest Texas Regional Advisory Council (STRAC) ID Card
Multi-Factor Authentication

❖ What you know
  ❖ password, passphrase, mother's maiden name

❖ What you have
  ❖ Smart card, OTP token

❖ What you are or what you do - biometrics
  ❖ Iris, finger print, face, voice, typing dynamics

❖ Authentications using more than one factors are called strong authentications
Identity Federation: Single Sign-On

1. User tries to access a service
2. Service providers delegates authentication to Identity Provider
3. Identity Provider authenticates user
4. Identity Provider retrieves user identity and attributes
5. Identity and attributes are returned to service provider
Secure Element and Privacy

- Secure vault for sensitive data
  - protect against theft

- Privacy cryptography
  - enable anonymous transactions
  - prevent tracking

- Only disclose the needed information

- Trusted offline transactions
Mobile Connect

- Uses your mobile device as your identity

- Services
  - Authentication
  - Transaction signing
  - Attributes sharing

- Federated identity service

- Various authentication mechanism transparent to the user.

- GSMA standard
Provide the **simplest user experience**

Press OK

Enter PIN code

Do you want to login to ft.com?

OK  Cancel

Please enter PIN to login to ft.com code:

OK  Cancel

Access Granted
Mobile Connect ecosystem

Tablet/desktop browser

End-user

Mobile device

SIM/UICC Card

Card Authentication Application

Service Provider

Discovery Provider

1. End-user

2. Tablet/desktop browser

3. Service Provider

4. Discovery Provider

5. Identity Gateway

6. Mobile device
Securing cars, infrastructure, and services

1. Authentication into diagnostic tool used by dealer and independent garages to issue new/replacement car keys.
2. Signing of tokens done with PKI and root in HSM
3. Issuance of RSA public keys and certificates to Electronic Control Units (ECU).
4. SE protects private keys and crypto processes.
5. Enable remote updates of firmware/software to ECUs in the field.
6. User authentication to the car – SE-based authentication
7. Communication to cellular network
Smart Metering Gateway

- **Gateway**
  - Firewall
  - Collects, processes and stores the records from Meter(s)
  - Access control
  - Meter Data encrypted and signed before sending

- **Security Module**
  - Cryptographic service provider
  - Secure storage

Assets to be protected:
- Meter Data
- System/Consumer log data
- Gateway time
- Personally Identifiable Information (PII)
- Configuration data (meters, gateway)
- Firmware
- Cryptographic keys
Takeaways

- Technology advances provide amazing benefits, productivity, and convenience
- Adversaries also use technologies to steal data and identities for financial gains and other malicious purposes
- Secure elements are effective tools for protecting our digital identities
Thank you!